FOS Networking Support

Dean Moore

17 January 1995

EOC LAN Primary Level 4 Requirements

Functionality

- The EOC LAN shall include a separate network for support functions that will not interfere with the operational network
- The Support Net architecture shall be identical in function and performance to that of the Operational Net

  (Support Net handles non-operational functions such as software testing and historical playback)

Performance

- The EOC Operational Net backbone shall be able to support a peak aggregate traffic rate of 20 Mb/s
- The EOC LAN must not inhibit the reconfiguration of EOC devices to perform Operational and Support functions

EOC LAN Primary Level 4 Requirements (cont.)

RMA

- The EOC Operational LAN shall be configured to support the following RMA requirements:

Critical Real-time data:	Availability = 0.9998	; MDT < 1 minute
Non-Critical Real-time data:	Availability = 0.99925	; MDT < 5 minute

- The EOC Operational LAN shall have no single-point of failure for critical real-time functions

- The EOC Support LAN shall have an operational availability of at least 0.96 and shall have a MDT of no greater than 4 hours

EOC LAN Primary Level 4 Requirements (cont.)

Scalability and Evolvability (covers through all releases)

- **The EOC Operational Net and Support Net shall be able to support 230 network devices without redesign**
- **The EOC Operational Net backbone shall be able to support peak data rates of up to 40 Mb/s without redesign**
- **The EOC LAN architecture shall support evolution to new technologies**

Security

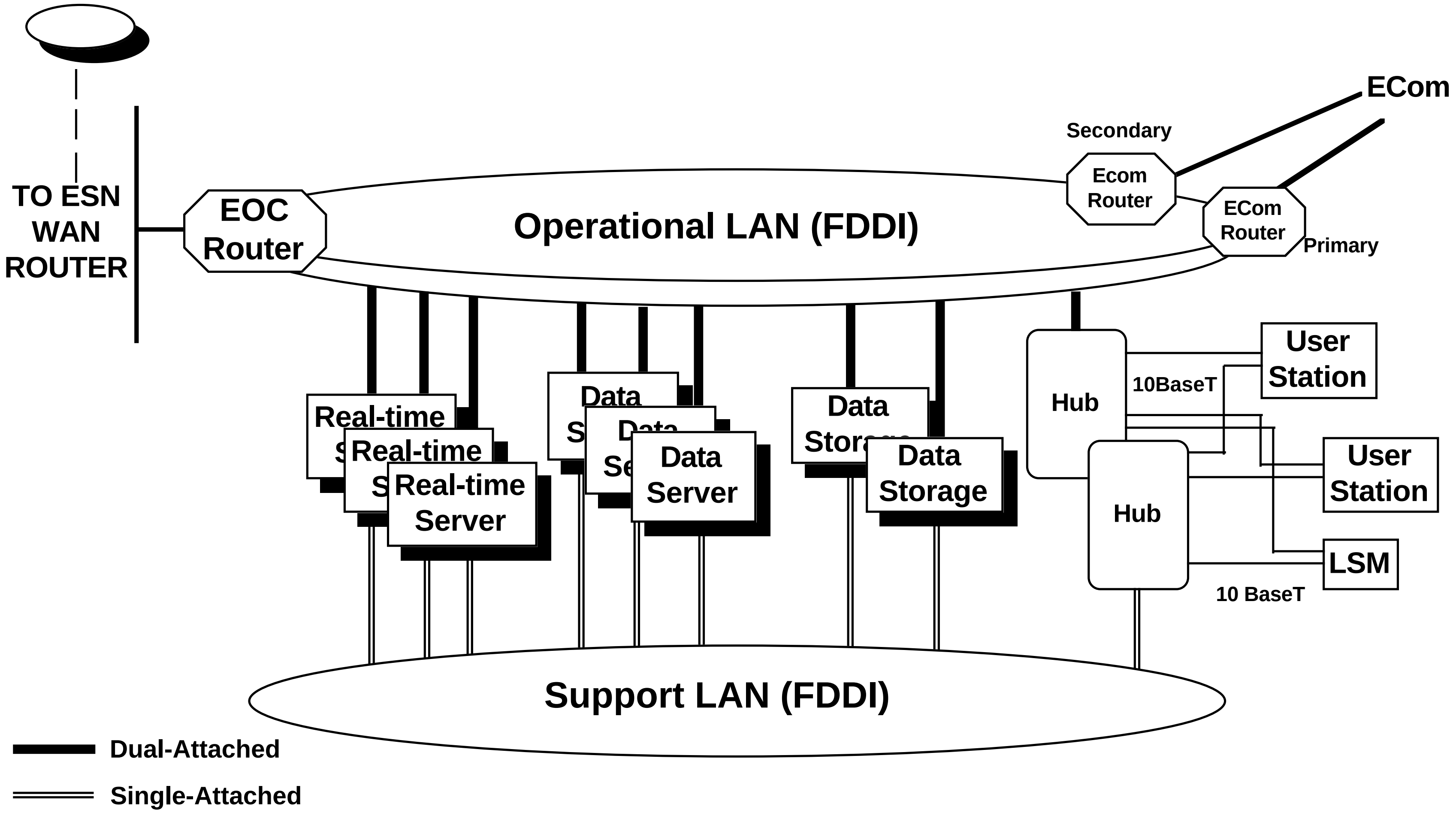
- **The EOC LAN shall be able to perform filtering based on network address, TCP socket number, and protocol to control access from external and internal interfaces (allows control of IST access)**

EOC LAN Preliminary Design

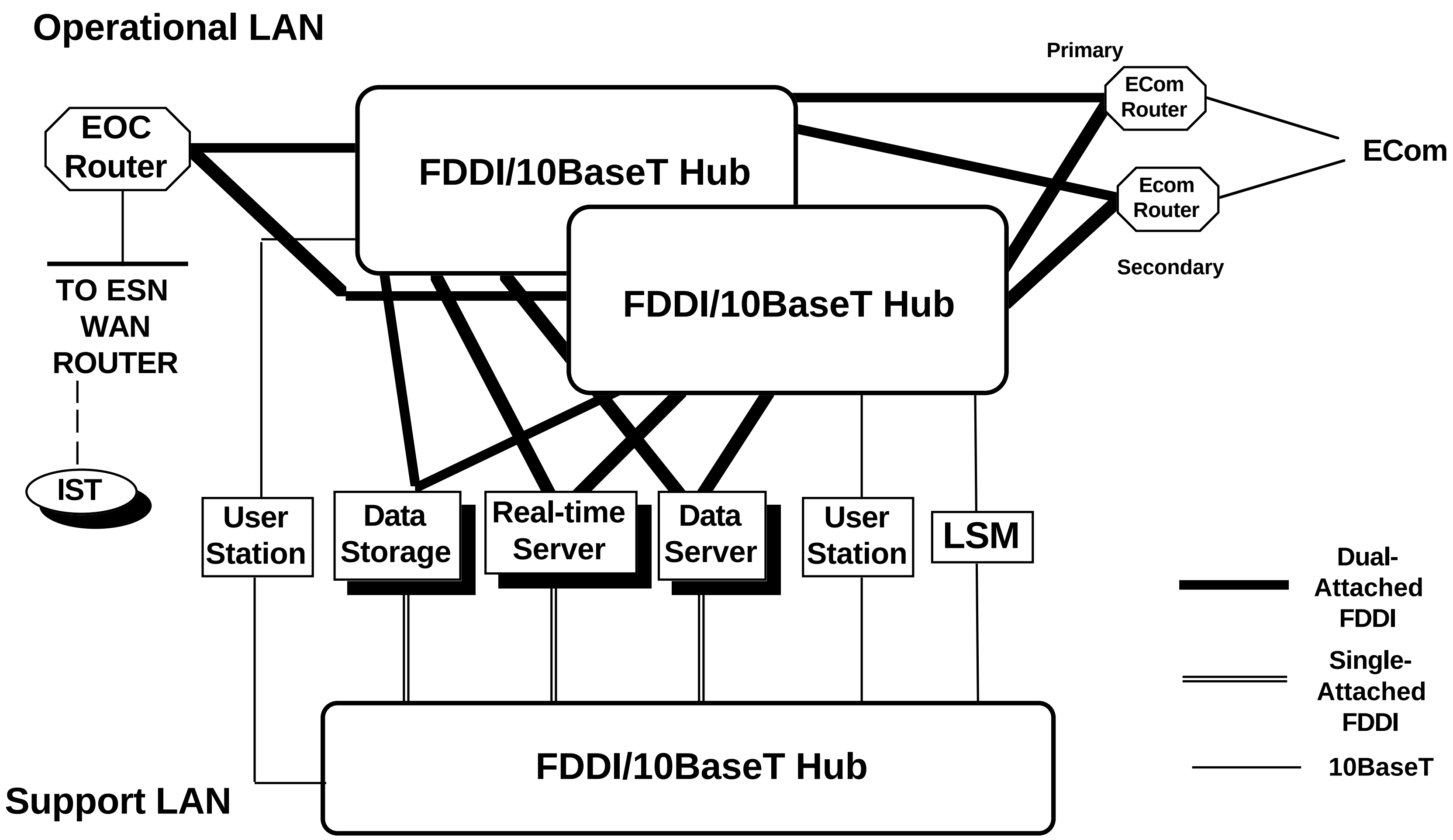
Design Utilizes Separate FDDI LANs for the Operational and Support Nets

- **Servers and Data Storage are attached to FDDI**
- **User Stations are attached to dedicated Ethernet segments**
- **All hosts attached to both Operational Net and Support Net**

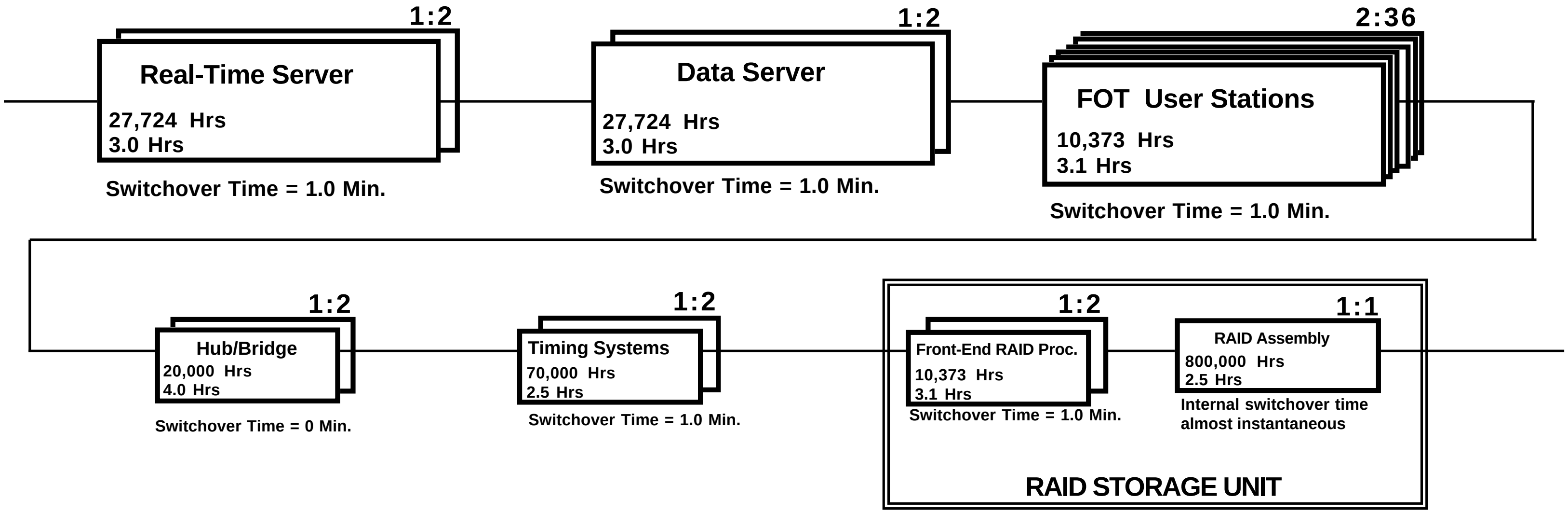
EOC LAN Design: Logical Connectivity



EOC LAN Design: Physical Connectivity



EOC Availability Modeling Results



Release A/B FOS Critical Real-Time Functions Hardware Reliability Block Diagram

Design Benefits

100 Mbps FDDI backbone provides plenty of bandwidth to handle future growth

Switched Ethernet provides each User Station with its own dedicated bandwidth not shared by other User Stations

Separate Operational and Support LANs provide efficient network utilization by segregating traffic

FDDI and Ethernet are “low risk” technologies

Attaching devices to both the Operational and Support LANs allows devices to switch function without reconfiguration of hardware (switch-over accomplished totally in software)

More Design Benefits

Flexible topology allows evolution of ops concept and data flows without necessitating network hardware modifications

Advantages of Hub Implementation:

- Allows hosts to be added without disrupting network operation
- Provides central monitoring and troubleshooting point
- Hubs “chained” together to allow expansion

Instrument Support Terminals

ISTs are analogous to EOC User Stations with a few exceptions

- Have no real-time command authority, but can issue command requests

Primary functionality

- Monitor real-time telemetry
- Analyze historical telemetry
- Modify and upload schedule activities

IST Connectivity Requirements and Assumptions

Network design must consider

- ISTs dispersed across campus areas (e.g., 6 CERES ISTs across 6 buildings on and off LaRC campus)
- ISTs not Co-Located with DAACs (e.g., University of Toronto)
- IST locations may change (due to office moves, department re-organizations, etc.)
- IST RMA applies to ECS domain only (e.g., for ECS-controlled systems)

These impact design by

- Reducing feasibility of dedicated net to IST hosts
- Increasing need for flexibility through use of existing campus-wide infrastructure

IST Traffic Flows

Worst Case

Site	# of AM-1 ISTs	Real-Time Telemetry (kbps)	Replay Traffic (kbps)
GSFC	3	249	894
JPL	3	249	894
LaRC	6	498	1788
NCAR	1	83	298
Canada	1	83	298
Japan (TBD)	TBD	TBD	TBD

Flows based on FOS User Profile

Site	Number of ISTs	Network	Bandwidth TO IST in kbps	Bandwidth FROM IST in kbps	Total to/from Bandwidth in kbps
GSFC (1)	3	ESN	659	58	717
JPL (1)	3	ESN	659	58	717
LaRC (2)	6	ESN	1,084	116	1,200
NCAR (3)	1	ESN	298	19	317
Canada (3)	1	NSI	298	19	317
Japan (TBD) (4)	TBD	TBD	TBD	TBD	TBD

IST Network Connectivity

Generic Solution for ISTs Co-Located with DAACs

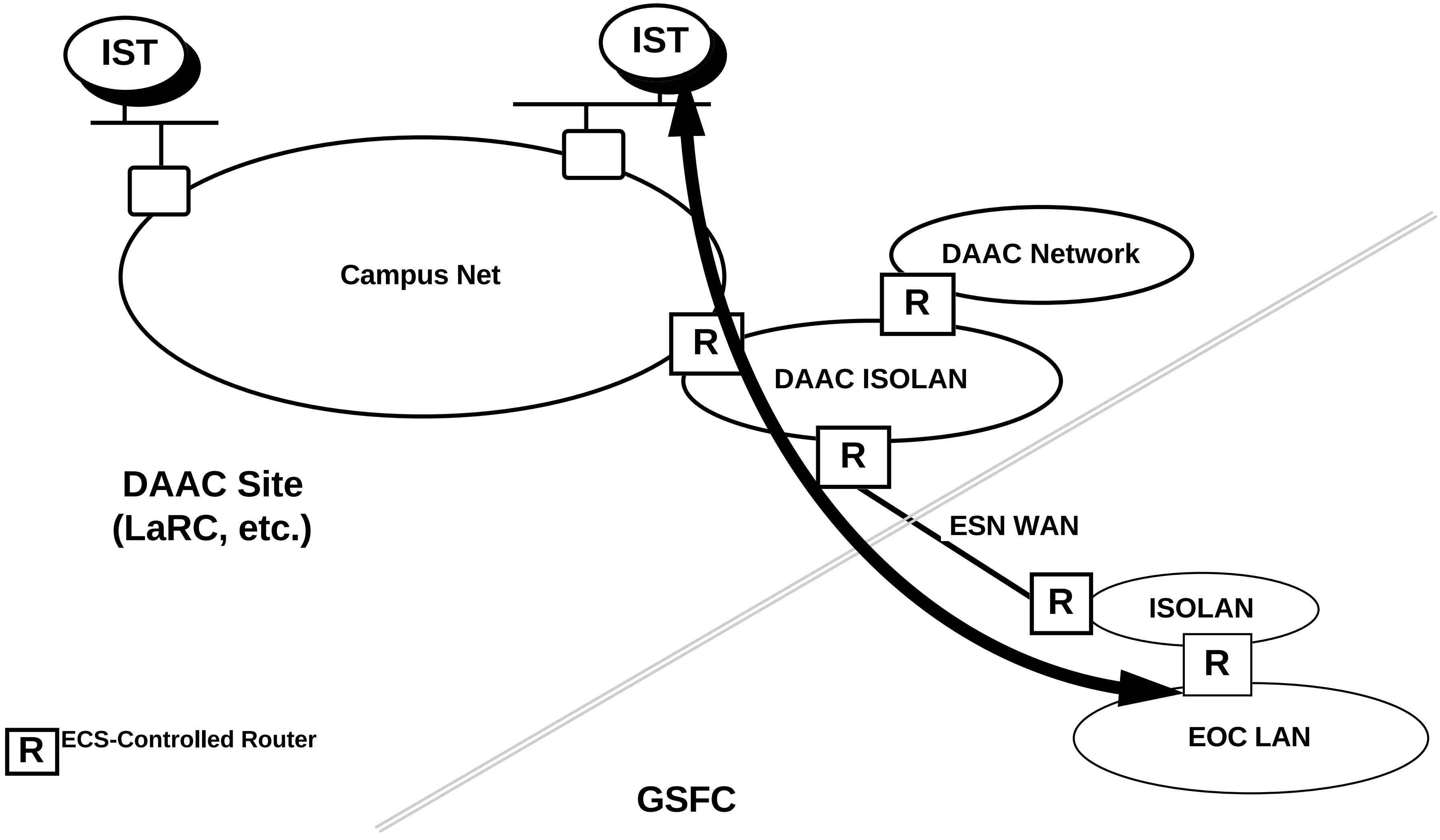
- ISTs will utilize the ESN WAN bandwidth from EOC to DAAC site
- ISTs will use the site campus network from ESN point-of-presence to the IST desktop
- If all ISTs in same location, providing dedicated network to IST “pool” will be considered
- Implementations will vary DAAC-by-DAAC (e.g., use dedicated nets, static routing scheme, etc.)

For ISTs Not Co-Located with DAACs (e.g., Univ. of Toronto)

- Use NSI or other Internet provider

Note: Release A involves IST early interface testing -- all ISTs do not appear until Release B

IST Network Connectivity (cont.)



Possible DAAC Implementations

LaRC

- Bridged campus topology means simplified path from ECS Router to IST
- Assign campus and ECS addresses to IST host
- IST part of ECS domain, eliminating need for static routes

JPL and GSFC

- Could assign ECS addresses to ISTs
- Assign ECS addresses to campus routers to extend ECS network to ISTs

IST Security Requirements

Because ISTs are part of campus/Internet environment, the following security is required:

- **Network security provided via filters on EOC routers**
- **Authentication and Authorization to prevent impersonation of legitimate users**
- **Data Integrity to insure data not modified during transit**

Analysis revealed

- **Software solutions provide better price/performance than hardware (smart card) solutions**
- **DCE effectively provides Authentication, Authorization, and Data Integrity**

IST Security Implementation

Security Need	Implementation
Authentication • Passwords do not appear on net	DCE-based Kerberos encryption
Authorization and Access Control • Integrated with Authentication • Network Layer • Application layer	DCE Access Control Lists (ACLs) and Router Firewalls at EOC
Data Integrity • Encrypted checksums (prevents intentional tampering and unintentional data corruption during transit)	DCE Remote Procedure Call (RPC)

FOS Multicasting

Reduces load on processors and network

Used to send real-time telemetry to User Stations and ISTs

CSMS analyzed and prototyped two options

- Reliable Multicast Protocol (RMP) -- relies on network-layer IP multicasting
- DCE Multicast RPCs -- application-layer multicasting

Other protocols (GTS, MTP, SCE, etc.) proposed but not implemented

- These may be evaluated if products become available

Analysis / prototyping revealed RMP to be the most promising

Reliable Multicast Protocol (RMP)

Provides ordered, reliable, fault-tolerant multicast service on top of unreliable multicast datagram service (such as IP multicasting)

RMP alone can multicast within a single LAN (e.g., EOC Operational Net)

Uses other protocols to multicast across routers/subnets (e.g., to ISTs)

- Multicast routers (e.g., using MOSPF or PIM) to route packets directly
- Otherwise, MBONE infrastructure using "mrouted" process to create multicast tunnels across nets

Issues

- Prototyping has revealed stability problems
- RMP not yet standardized (expected end of 1995)
- Network topology may complicate multicasting to ISTs